UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	16-cr-798 (KBF)
- v. -	OPINION & ORDER
NIMESH PATEL,	
Defendant.	

KATHERINE B. FORREST, United States District Judsge:

Currently before the Court is defendant Nimesh Patel's motion, pursuant to Fed. R. Crim. P. 41(e), demanding the return of property that the Government obtained during the course of an allegedly unlawful search and seizure and seeking an order prohibiting the Government from using such materials at trial. (See ECF No. 31 at 5.) For the reasons set forth below, Patels' motion is DENIED.

I. BACKGROUND[1]

Nimesh Patel was a Senior Director for Systems at the Leukemia and Lymphoma Society ("LLS") from January 2006 until October 2014. In February 2009, LLS entered into a contractual relationship with Pyramid Technology Solutions, Inc. ("Pyramid"). The government contends that between September 2012 and September 2014, Patel awarded LLS contracts to Pyramid in exchange for $274,000 in kickbacks, which were allegedly paid by Patel's co-defendant, Dilip Vadlamudi, to a shell company controlled by Patel.

[1] All parties agree that the facts underlying this motion are not in dispute. (See ECF No. 38.) The facts described herein are drawn from the parties' respective briefing. (See ECF Nos. 31, 34.)

On March 30, 2016, law enforcement agents served Patel and Vadlamudi with subpoenas directed to the co-defendants' respective companies—Dots Consulting, Inc. (for Patel) and Idealogix, LLC (for Vadlamudi). Among the documents that counsel for Dots Consulting, Inc. and Patel produced in response to the subpoeans were emails from two accounts affiliated with Patel—dotsconsulting@gmail.com and nimesph@hotmail.com.

On June 10, 2016, acting pursuant to an affidavit submitted by a U.S. Postal Inspector and under the auspices of the Stored Communications Act, 18 U.S.C. §§ 2703, U.S. Magistrate Judge Kevin Nathaniel Fox issued warrants to Google, Inc., Yahoo! Inc., and Microsoft Corporation directing those providers to produce all emails sent, received or created between October 1, 2012 and June 10, 2016 in connection with certain email accounts, including dotsconsulting@gmail.com and nimeshp@hotmail.com. The warrants authorized law enforcement personnel to review the production for evidence, fruits and instrumentalities of certain enumerated offenses. The warrants specified the types of materials that would constitute "evidence, fruits, and instrumentalities" of the subject offenses. The service providers complied with the warrants and produced the contents of the two subject email accounts to U.S. Postal Inspector agents, who then used keyword searches on the emails to identify responsive materials.

On December 5, 2016, Patel and Vadlamudi were indicted for conspiring to commit honest services wire fraud, conspiring to violate the Travel Act and conspiring to commit money laundering. The government began producing

materials to the defense thereafter. On December 21, 2016, the Government produced to both defendants' counsel the warrants and the warrant application, and also emailed a proposed protective order to defense counsel, which all parties signed on December 28, 2016. The protective order provided that "information that may be subject to disclosure in this case" may be contained in emails that were seized during the course of the investigation. The protective order further provided that the Government would "disclose to counsel for the defendants . . . the entirety of such seized [electronically seized information] as the Government believes may contain disclosure material." On December 30, 2016, the Government produced to both defendants the contents of the email accounts that were seized pursuant to the June 10 warrants.

Patel's counsel subsequently informed the Government that he believed the contents of the email accounts dotconsulting@gmail.com and nimeshp@hotmail.com contained material protected by the attorney-client privilege. The Government then established a "wall" review wherein an Assistant U.S. Attorney not connected with the investigation or prosecution of the case reviewed the accounts using search terms and filtered out privileged emails. The reviewing Assistant U.S. Attorney then provided all non-privileged materials in the accounts to the prosecuting team, who, in turn, provided that whittled down version of the accounts to both defendants.

Patel now argues that the June 10 warrants, which authorized seizure of all emails sent, received or created by the two subject emails accounts between October

1, 2012 and June 10, 2016 violated the Fourth Amendment's particularity requirement by authorizing the Government to seize "every email ever written by Nimesh Patel even months after he'[d] ceased to be employed by the Leukemia and Lymphoma Society." (ECF No. 31 at 7.) In addition, Patel contends that the Government violated his attorney-client privilege by releasing the full contents of his email accounts to his co-defendant on December 30, 2016. (Id. at 12.) Patel insists that such a violation would have been avoided had the Government contained its search warrant request to the time of Patel's employment with LLS or vetted the emails before releasing them. (Id. at 5.) As a remedy, Patel seeks the return of all the seized materials and an order prohibiting the Government from using any of the materials seized pursuant to the June 10 warrants at trial. (See id.) Patel's motion is DENIED.

II. THE JUNE 10 WARRANTS' PARTICULARITY

A. Legal Standard

1. Particularity

The Fourth Amendment protects against "general, exploratory rummaging in a person's belongings," Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971), by requiring search warrants to describe with particularity the materials the Government seeks to seize, see Marron v. United States, 275 U.S. 192, 196 (1927). In general, a warrant is sufficiently particular if it "enable[s] the executing officer to ascertain and identify with reasonable certainty those items that the magistrate has authorized him to seize." United States v. George, 975 F.2d 72, 75 (2d Cir.

1992). "The degree to which a warrant must state its terms with particularity varies inversely with the complexity of the criminal activity investigated." United States v. Regan, 706 F. Supp. 1102, 1113 (S.D.N.Y. 1989). Thus, "where a particularly complex scheme is alleged to exist, it may be appropriate to use more generic terms to describe what is to be seized." United States v. Gotti, 42 F. Supp. 2d 252, 274 (S.D.N.Y. 1999) (citing Regan, 706 F. Supp. at 1113).

Under the exclusionary rule, the remedy for searches and seizures conducted pursuant to a constitutionally defective warrant is suppression. United States v. Leon, 468 U.S. 897, 906 (1984). However, the exclusionary rule "operates as 'a judicially created remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect, rather than a personal constitutional right of the party aggrieved,'" id. (quoting United States v. Calandra, 414 U.S. 338, 348 (1974)), and it applies only when the deterrence benefits of suppression outweigh the rule's heavy costs, Davis v. United States, 564 U.S. 229, 240 (2011) ("Police practices trigger the harsh sanction of exclusion only when they are deliberate enough to yield 'meaningful[]' deterrence, and culpable enough to be 'worth the price paid by the justice system.'" (quoting Herring v. United States, 555 U.S. 135, 144 (2009))).

Reasonable reliance on a judicially authorized warrant—even if that warrant is later held invalid—does not constitute the sort of "'deliberate,' 'reckless,' or 'grossly negligent' disregard for Fourth Amendment rights" that the exclusionary rule was meant to deter. See Davis, 564 U.S. at 238 (quoting Herring, 555 U.S. at

144). Accordingly, such reasonable reliance constitutes a "good faith" defense to the rule's application, and suppression is not appropriate. See id. at 240 ("[W]e have 'never applied' the exclusionary rule to suppress evidence obtained as a result of nonculpable, innocent police conduct." (quoting Herring, 555 U.S. at 144)). Reliance on a judicially authorized warrant is unreasonable only when (1) "the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth," Leon, 468 U.S. at 923, (2) the magistrate "wholly abandoned his judicial role," id., (3) the affidavit was "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable," id. (quoting Brown v. Illinois, 422 U.S. 590, 611 (1975) (Powell, J., concurring), or (4) the warrant was "so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid," id.

2. Stored Communications Act

Under the Stored Communications Act, the Government "may require a provider of remote computing service to disclose the contents of any wire or electronic communication" without first providing notice to the subscriber or customer, if the Government obtains a warrant using the procedures described in the Federal Rules of Criminal Procedure. 18 U.S.C. §§ 2703(b). Searches for and seizures of electronic evidence pose unique Fourth Amendment challenges, as such evidence "typically consists of enormous amounts of undifferentiated information and documents." In the Matter of a Warrant for All Content & Other Info.

Associated with the Email Account xxxxxxx gmail.com Maintained at Premises Controlled By Google, Inc., 33 F. Supp. 3d 386, 392 (S.D.N.Y. 2014), as amended (Aug. 7, 2014). As a result, courts have developed "a more flexible approach to the execution of search warrants for electronic evidence, holding the government to a standard of reasonableness." United States v. Metter, 860 F. Supp. 2d 205, 214 (E.D.N.Y. 2012).

Given the enormity of the data contained on computers or in email accounts, courts have repeatedly recognized that "a search for [electronic] documents or files responsive to a warrant cannot possibly be accomplished during an on-site search." In the Matter of a Warrant, 33 F. Supp. 3d at 392; see also Metter, 860 F. Supp. 2d at 214 ("The Court does not expect the government to make onsite determinations of whether a file or document contained on a hard drive or in an email account falls within the scope of the warrant and, thus, off-site imagining is a necessity of the digital era."). Instead, "'it is frequently the case with computers that the normal sequence of "search" and then selective "seizure" is turned on its head,' as computer hardware is seized from a suspect's premises before its content is known and then searched at a later time." United States v. Vilar, No. S305CR621KMK, 2007 WL 1075041, at *35 (S.D.N.Y. Apr. 4, 2007) (quoting In re Search of 3817 W. W. End, First Floor Chicago, Illinois 60621, 321 F. Supp. 2d 953, 958 (N.D. Ill. 2004)); see also In the Matter of a Warrant, 33 F. Supp. 3d at 394 ("We perceive no constitutionally significant difference between the searches of hard drives just discussed and searches of email accounts."). Accordingly, when armed with a

search warrant describing with particularity the types of emails to be searched, the Government may obtain the entire contents of an email account and then conduct a review to determine which emails fall within the warrant's scope. United States v. Bowen, 689 F. Supp. 2d 675, 682 (S.D.N.Y. 2010), aff'd sub nom. United States v. Ingram, 490 F. App'x 363 (2d Cir. 2012) (holding that the Fourth Amended does not require executing authorities "to delegate a pre-screening function to the internet service provider or to ascertain which e-mails are relevant before copies are obtained from the internet service provider for subsequent searching").

This does not mean, however, that the Fourth Amendment's particularity requirement falls away when dealing with electronic evidence. "There is . . . one form of particularity whose absence the Second Circuit has unequivocally and unqualifiedly condemned: '[A]uthorization to search for evidence of a crime, that is to say, any crime, is so broad as to constitute a general warrant.'" United States v. Cioffi, 668 F. Supp. 2d 385, 392 (E.D.N.Y. 2009) (quoting United States v. George, 975 F.2d 72, 76 (2d Cir. 1992)) (alteration in original). Thus, where a warrant does not, either on its face or via incorporation of a supporting affidavit, "limit the items to be seized from [a defendant's] personal email account to emails containing evidence of the crimes charged in the indictment," the warrant will not be considered constitutionally valid. See id. at 396.

Taken together, then, the above principles make clear that executing authorities may obtain the entire contents of an email account in an effort to search for a more limited set of emails. In so doing, the Government may engage in "some

perusal, generally fairly brief, of . . . documents (seized during an otherwise valid search) . . . in order for the police to perceive the relevance of the documents to crime." United States v. Mannino, 635 F.2d 110, 115 (2d Cir. 1980) (quoting United States v. Ochs, 595 F.2d 1247, 1257 n.8 (2d Cir. 1979)) (internal quotation marks omitted) (alterations in original); accord Andresen v. Maryland, 427 U.S. 463, 482 n. 11 (1976) ("In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized.").

B. Discussion

Patel insists that the June 10 warrants were insufficiently particularized because they authorized the government to seize "every email ever written by Nimesh Patel even months after he'[d] ceased to be employed by the Leukemia and Lymphoma Society" (see ECF No. 31 at 7), and offered no "guidelines to aid the determination of what may or may not be seized" (id. at 9 (citing United States v. Cardwell, 680 F.2d 75, 78 (9th Cir. 1982)) (internal quotation marks omitted).) To the extent Patel takes issue with the Government's collection of his entire email account rather than a specified subset of emails, his objections are premised on a misapplication of the law. As the Court has detailed above, courts have long recognized that "the normal sequence of "search" and then selective "seizure" is turned on its head" with regard to electronically stored data. See Vilar, 2007 WL 1075041, at *35 (quoting W. W. End, 321 F. Supp. 2d at 958); cf. United States v. Ganias, 755 F.3d 125, 135 (2d Cir. 2014) ("[T]he creation of mirror images [of

computer hard drives] for offsite review is constitutionally permissible in most instances, even if wholesale removal of tangible papers would not be."). A warrant therefore does not violate the Fourth Amendment's particularity requirement where it permits the Government "to obtain the entire contents of the email account to determine which particular emails come within the search warrant." In the Matter of a Warrant, 33 F. Supp. 3d at 394.

Patel's subsidiary argument—that the warrant failed to limit the subject matter of the search—also fails. The warrants specifically authorized law enforcement personnel "to review the records produced by [Google, Yahoo and Microsoft] in order to locate any evidence, fruits, and instrumentalities" of five specific offenses (wire fraud, honest services wire fraud, conspiracy to commit wire fraud and honest services wire fraud, money laundering and conspiracy to commit money laundering). (ECF No. 34, Ex. 1, Warrant, Email Search Attachment A at 2.) The warrants then stated that evidence, fruits and instrumentalities of those six enumerated offenses "includ[e] the following" nine categories of documents: evidence of crime; preparation of crime; state of mind; user identity; timeline; geographic location of use, computer, or device; identities and locations of co-conspirators; location of other evidence; and passwords or other information needed to access user's computer or other online accounts. (Id. at 2-3) Finally, the warrants provided examples of documents that would fall within each of the nine document categories. (Id.)

"Generally, a warrant that authorizes a search for documents or things that constitute evidence of a particular crime is not overbroad; rather, 'generic terms may be used to describe the materials to be seized so long as the warrant identifies a specific illegal activity to which the item related.'" United States v. Lebovits, No. 11-CR-134 SJ, 2012 WL 10181099, at *23 (E.D.N.Y. Nov. 30, 2012) (quoting United States v. Lake, 233 F. Supp. 2d 465, 471 (E.D.N.Y. 2002)), report and recommendation adopted, No. 11 CR 134 SJ, 2014 WL 201495 (E.D.N.Y. Jan. 16, 2014), and report and recommendation adopted sub nom., United States v. Gutwein, No. 11 CR 134 SJ, 2014 WL 201500 (E.D.N.Y. Jan. 16, 2014). Though the nine document categories were not introduced as an exhaustive list of the documents covered by the warrants (in that the warrants authorized law enforcement personnel to locate "any evidence, fruits and instrumentalities [of the six enumerated offense], including the following" document types (see ECF No. 34, Ex. 1, Warrant, Email Search Attachment A at 2 (emphasis added))), this modicum of vagueness does not render the warrants invalid. As much is clear from the Second Circuit's opinion in United States v. Riley, 906 F.2d 841 (2d Cir. 1990):

> In upholding broadly worded categories of items available for seizure, we have noted that the language of a warrant is to be construed in light of an illustrative list of seizable items. In the pending case, the warrant supplied sufficient examples of the type of records that could be seized—bank records, business records, and safety deposit box records. No doubt the description, even with illustrations, did not eliminate all discretion of the officers executing the warrant, as might have occurred, for example, if the warrant authorized seizure of the records of defendant's account at a named bank. But the particularity requirement is not so exacting. Once a category of seizable papers has been adequately described, with the description delineated in part by an illustrative list of seizable items, the Fourth Amendment is not

> violated because the officers executing the warrant must exercise some minimal judgment as to whether a particular document falls within the described category.

Id. at 844-45; see also United States v. Bazzi, No. 07-CR-212 A M, 2010 WL 4451454, at *23 (W.D.N.Y. Apr. 21, 2010) (denying motion to suppress where "the search warrant used the language 'included but not limited to' in describing the categories of items that could be seized, [but] it instructed that any item seized 'must relate to violations'" of specific enumerated offenses (citation omitted)), report and recommendation adopted sub nom. United States v. Xu Hang Wang, No. 07-CR-212A, 2010 WL 4451244 (W.D.N.Y. Nov. 3, 2010).

Finally, Patel appears to argue that the warrant was improper because there was not sufficient probable cause to believe that emails sent, received or drafted after Patel's employment at LLS would lead to evidence of criminality. Though Patel's argument on this point is not clearly articulated, he suggests, as the defendant did in In the Matter of a Warrant, that it was inappropriate "to issue a search warrant that allows the Government to obtain all emails in an account even though there is no probable cause to believe that the email account consists exclusively of emails that are within the categories of items to be seized under the search warrant." See 33 F. Supp. 3d at 390. While the Court is hesitant to address an argument that Patel has not himself clearly raised, it suffices to say that "the magistrate's finding of probable cause is entitled to substantial deference"; "the magistrate's finding of probable cause is itself a substantial factor tending to uphold the validity of [a] warrant"; and "doubts should be resolved in favor of upholding the

warrant." United States v. Travisano, 724 F.2d 341, 345 (2d Cir. 1983) (citations omitted). Here, the Court has no difficulty upholding the magistrate's finding of probable cause with regard to emails drafted or received after October 2014 (when Patel's employment with LLS terminated), particularly since the affidavit submitted in support of the Government's warrant application noted that Patel and Vadlamudi had continued to exchange emails until at least February 18, 2016—i.e., sixteen months after Patel left LLS. (See ECF No. 34, Ex. 1, Agent Affidavit at 8 ("Between on or about December 11, 2009 and on or about February 18, 2016, PATEL and VADLAMUDI exchanged approximately 3,096 emails.").) And, in any event, the executing authorities "manifest[ed] objective good faith in relying on [the June 10] warrant[s]," as the warrant was not "based on an affidavit 'so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable.'" Leon, 468 U.S. at 923 (quoting Brown, 422 U.S. at 611). There is therefore no basis for suppression on these grounds.

III. ATTORNEY-CLIENT PRIVILEGE

Patel urges the Court to order blanket suppression of all materials seized pursuant to the June 10 warrants based on the Government's seizure of the email accounts and its subsequent disclosure of purportedly privileged materials to Patel's co-defendant. (ECF No. 31 at 5.) Patel argues that the Government failed to take "any initial measures of caution" to avoid releasing privileged materials, as evidenced by (1) seeking and obtaining a warrant that reached emails sent and received between October 1, 2012 and June 10, 2016, even though the Government

knew Patel's employment at LLS had ended in October 2014 and that his legal representation began as early as April 25, 2016; and (2) failing to "simply vet the emails by searching for counsel's email domain name in a search of the emails prior to releasing them." (ECF No. 31 at 4-5, 12.) According to Patel, the Government's release of privileged materials to Vadlamudi was not simply the result of "forgivable mistake or inadvertence," but instead caused him "irreparable harm" because there is no way to now know "how the insight gleaned from Mr. Patel's privileged emails contributed to codefendant, Dilip Vadlamudi's decision to plead guilty." (Id. at 1, 10, 12.)

Indisputably, when the Government obtains access to a defendant's email account, the Government is not entitled to rely on privileged materials contained therein. See United States v. Nunez, No. 12 CR. 778-2, 2013 WL 4407069, at *1, *3 (S.D.N.Y. Aug. 16, 2013) (in case concerning suppression of privileged emails that were seized pursuant to warrant authorizing Government to "receiv[e] the contents of the [defendant's] Gmail Account from Google," court found that "the Government's investigation or prosecution of [defendant] would be prejudiced by the suppression of thee [p]otentially [p]rivileged [e]mails, beyond the deprivation of information to which it was not originally entitled"). But "'[t]he general remedy for violation of the attorney-client privilege is to suppress introduction of the privileged information at trial,' not to order wholesale suppression." United States v. Lumiere, No. 16 CR. 483, 2016 WL 7188149, at *6 (S.D.N.Y. Nov. 29, 2016) (quoting United States v. SDI Future Health, Inc., 464 F. Supp. 2d 1027, 1047 (D. Nev. 2006)); see

also Nat'l City Trading Corp. v. United States, 635 F.2d 1020, 1026 (2d Cir. 1980) ("To the extent that the files obtained . . . were privileged, the remedy is suppression and return of the documents in question, not invalidation of the search.") (internal citations omitted). Neither Patel nor the Government has identified any instances where a court authorized blanket suppression or invalidation of a search warrant following seizure of privileged material.

A sister court's recent decision in Lumiere is particularly instructive. There, as here, a defendant whose electronic devices had been seized pursuant to a search warrant argued that "blanket suppression [of the evidence gleaned from those devices was appropriate] because the Government [had] adopted no precautions against viewing privileged documents in its search of [defendant's] devices, despite being on notice of attorney-client communications." 2016 WL 7188149, at *6. Relying on Second Circuit case law, the Lumiere court noted that "[t]he 'drastic remedy of the suppression of all evidence is not justified unless those executing the warrant acted "in a flagrant disregard" of the warrant's terms.'" Id. at *5 (quoting United States v. Matias, 836 F.2d 744, 747 (2d Cir. 1988)). "Government agents flagrantly disregard the terms of a warrant so that wholesale suppression is required only when (1) they effect a widespread seizure of items that were not within the scope of the warrant and (2) do not act in good faith." Id. (quoting United States v. Shi Yan Liu, 239 F.3d 138, 140 (2d Cir. 2000)) (internal quotation marks omitted).

Guided by those background principles, the Lumiere court "evaluated [the defendant's] novel argument under the 'general touchstone of reasonableness which governs Fourth Amendment analysis.'" Id. (quoting United States v. Ramirez, 523 U.S. 65, 71 (1998)). In finding that the Government's handling of the defendant's seized devices was reasonable, the court noted that (1) the Government had completed its review of the seized devices before being notified that the devices might contain significant numbers of privileged documents; (2) at the time of the devices' seizure, the Government was only aware of one attorney representing the defendant, and therefore avoiding privileged materials required nothing more "than keep[ing] an eye out for [the attorney's name]; (3) the Government did not "revisit" the electronic evidence after receiving the notification; and (4) the Government's review was "consistent with the warrant," in that the warrant did not mandate any special procedures for avoiding privileged documents. Id. at *6-7.

As in Lumiere, this Court finds that the Government's conduct does not justify blanket suppression of all emails seized pursuant to the June 10 warrants. Nothing in the warrant—which the Court has already found to be proper in all respects—required the U.S. Postal Inspection Service (the government investigative agency that received the records produced pursuant to the warrant (see ECF No. 34, Ex. 1, Warrant)) to establish a review protocol ex ante to segregate privileged emails. As a result, the Government's review protocol, or lack thereof, did not run afoul of the warrant's requirements. In addition, upon receiving notice that the accounts contained significant numbers of privilege materials, the Government

established a "wall" review wherein a U.S. Attorney not affiliated with the investigation or prosecution of the matter reviewed the emails using search terms and filtered out privileged items before returning the unprivileged portions of the email accounts to the prosecution team and the defense. (See ECF No. 34 at 4.) Such remedial steps do not evidence the sort of bad faith or flagrant disregard of the warrant's limits that would justify the wholesale suppression of evidence. Cf. Lumiere, 2016 WL 7188149, at *6 ("[A]fter-the-fact notice of potentially privileged documents did not render the Government's earlier search unreasonable.").

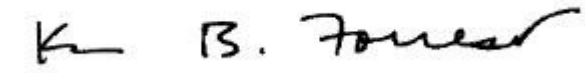
Moreover, to the extent Patel argues that the Government acted recklessly by failing to screen for privileged emails before providing them to Patel's co-defendant, the timing of the Protective Order vis-à-vis the Government's disclosure lessens the force of his claim. As explained above, before beginning production of the emails the Government provided a Protective Order to defendants, which both defendants signed, in which the Government stated that it had collected "electronic mail of Nimesh Patel and Dilip Vadlamudi" and notified defendants that it would "disclose to counsel for the defendants, for use solely as permitted herein, the entirety of such seized ESI [electronically stored information] as the Government believes may contain disclosure material." (ECF No. 34 at 12 n.2 (emphasis added).) The Protective Order therefore placed defendants on notice that the "entirety of [the] seized ESI" may be disclosed. Such notification provided defendants with an opportunity to raise their concerns regarding privileged materials at that time, and

thereby undermines any suggestion that the Government acted in bad faith when it ultimately released the privileged materials.

Ultimately, the "Government's review need only be reasonable, not perfect, and law enforcement is given significant latitude in determining how to execute a warrant." Lumiere, 2016 WL 7188149, at *6 n.9 (citing United States v. Salameh, 54 F. Supp. 2d 236, 277 (S.D.N.Y. 1999), aff'd, 16 F. App'x 73 (2d Cir. 2001)). As the case progresses, Patel may move to suppress any allegedly privileged materials that the Government seeks to introduce at trial, or may request a hearing to determine whether "information derived from [privileged] sources was used by the government, in violation of the attorney-client privilege, to prepare for trial." See United State v. Schwimmer, 892 F.2d 237, 244-45 (2d Cir. 1989). But plaintiffs' current request for blanket suppression of all evidence gathered from the June 10 warrants is DENIED.

SO ORDERED:

Dated: New York, New York
August 8, 2017



KATHERINE B. FORREST
United States District Judge